

WHAT IS CLAIMED IS:

1. A transmitting device for transmitting copyright  
protected contents data to a receiving device through radio  
5 communications, transmitting device comprising:

a first authentication unit configured to carry out a  
first authentication with the receiving device, for judging  
whether the receiving device is a device that is allowed to  
communicate with the transmitting device or not, on a radio  
10 link layer of the radio communications;

a first key exchange unit configured to generate a  
first encryption key and share the first encryption key  
with the receiving device when the first authentication  
with the receiving device by the first authentication unit  
15 is success;

a second authentication unit configured to carry out a  
second authentication with the receiving device, for  
protecting copyright of the contents data to be  
transmitted, through an encrypted radio communication using  
20 the first encryption key;

a second key exchange unit configured to generate a  
second encryption key and share the second encryption key  
with the receiving device when the second authentication  
with the receiving device by the second authentication unit  
25 is success; and

a communication unit configured to transmit the  
contents data to the receiving device through an encrypted  
communication path which is encrypted by using the second  
encryption key and provided on the radio link layer.  
30

2. The transmitting device of claim 1, wherein when the  
second authentication or sharing of the second encryption  
key is failure for a reason that the encrypted radio  
communication on the radio link layer is missing, one of  
35 the second authentication unit and the second key exchange



unit notifies the failure and the reason to the receiving device.

3. The transmitting device of claim 1, further comprising  
5 a storage unit configured to store the contents data.

4. The transmitting device of claim 1, wherein the first authentication by the first authentication unit is success when a PIN code entered at the transmitting device and a  
10 PIN code notified from the receiving device are in a prescribed relationship.

5. The transmitting device of claim 4, wherein each PIN code contains at least one of a varying code information, a  
15 prescribed code information, a body information acquired from a body of a user, and an attribute information regarding attributes of the user.

6. A transmitting device for transmitting copyright  
20 protected contents data to a receiving device through radio communications, transmitting device comprising:

a first authentication unit configured to carry out a first authentication with the receiving device, for judging whether the receiving device is a device that is allowed to  
25 communicate with the transmitting device or not, on a radio link layer of the radio communications;

a first key exchange unit configured to generate a first encryption key and share the first encryption key with the receiving device when the first authentication  
30 with the receiving device by the first authentication unit is success;

a second authentication unit configured to carry out a second authentication with the receiving device, for protecting copyright of the contents data to be  
35 transmitted, through an encrypted radio communication using

the first encryption key;

a second key exchange unit configured to generate a second encryption key and share the second encryption key with the receiving device when the second authentication  
5 with the receiving device by the second authentication unit is success; and

a communication unit configured to set up an encrypted communication path which is encrypted by using the second encryption key on the encrypted radio  
10 communication which is encrypted by using the first encryption key, and transmit the contents data to the receiving device through the encrypted communication path.

7. The transmitting device of claim 6, wherein when the  
15 second authentication or sharing of the second encryption key is failure for a reason that the encrypted radio communication on the radio link layer is missing, one of the second authentication unit and the second key exchange unit notifies the failure and the reason to the receiving  
20 device.

8. The transmitting device of claim 6, further comprising a storage unit configured to store the contents data.

9. The transmitting device of claim 6, wherein the first authentication by the first authentication unit is success when a PIN code entered at the transmitting device and a PIN code notified from the receiving device are in a prescribed relationship.  
30

10. The transmitting device of claim 9, wherein each PIN code contains at least one of a varying code information, a prescribed code information, a body information acquired from a body of a user, and an attribute information  
35 regarding attributes of the user.

11. A receiving device for receiving copyright protected contents data transmitted from a transmitting device through radio communications, the receiving device

5 comprising:

a first authentication unit configured to carry out a first authentication with the transmitting device, for enabling the receiving device to operate as a device that is allowed to communicate with the transmitting device, on  
10 a radio link layer of the radio communications;

a first key exchange unit configured to generate a first encryption key and share the first encryption key with the transmitting device when the first authentication with the transmitting device by the first authentication  
15 unit is success;

a second authentication unit configured to carry out a second authentication with the transmitting device, for protecting copyright of the contents data to be transmitted, through an encrypted radio communication using  
20 the first encryption key;

a second key exchange unit configured to generate a second encryption key and share the second encryption key with the transmitting device when the second authentication with the transmitting device by the second authentication  
25 unit is success; and

a communication unit configured to receive the contents data transmitted from the transmitting device through an encrypted communication path which is encrypted by using the second encryption key and provided on the  
30 radio link layer.

12. The receiving device of claim 11, further comprising a reproduction unit configured to reproduce the contents data.

35

13. The receiving device of claim 11, wherein the first authentication by the first authentication unit is success when a PIN code entered at the receiving device and a PIN code notified from the transmitting device are in a prescribed relationship.

14. The receiving device of claim 13, wherein each PIN code contains at least one of a varying code information, a prescribed code information, a body information acquired from a body of a user, and an attribute information regarding attributes of the user.

15. A receiving device for receiving copyright protected contents data transmitted from a transmitting device through radio communications, the receiving device comprising:

a first authentication unit configured to carry out a first authentication with the transmitting device, for enabling the receiving device to operate as a device that is allowed to communicate with the transmitting device, on a radio link layer of the radio communications;

a first key exchange unit configured to generate a first encryption key and share the first encryption key with the transmitting device when the first authentication with the transmitting device by the first authentication unit is success;

a second authentication unit configured to carry out a second authentication with the transmitting device, for protecting copyright of the contents data to be transmitted, through an encrypted radio communication using the first encryption key;

a second key exchange unit configured to generate a second encryption key and share the second encryption key with the transmitting device when the second authentication with the transmitting device by the second authentication

unit is success; and

5 a communication unit configured to set up an encrypted communication path which is encrypted by using the second encryption key on the encrypted radio communication which is encrypted by using the first encryption key, and receive the contents data transmitted from the transmitting device through the encrypted communication path.

10 16. The receiving device of claim 15, further comprising a reproduction unit configured to reproduce the contents data.

15 17. The receiving device of claim 15, wherein the first authentication by the first authentication unit is success when a PIN code entered at the receiving device and a PIN code notified from the transmitting device are in a prescribed relationship.

20 18. The receiving device of claim 17, wherein each PIN code contains at least one of a varying code information, a prescribed code information, a body information acquired from a body of a user, and an attribute information regarding attributes of the user.

25 19. A radio communication system, comprising a transmitting device for transmitting copyright protected contents data through radio communications, and a receiving device for receiving the contents data transmitted from the transmitting device, each one of the transmitting device and the receiving device having:

30 a first authentication unit configured to carry out a first authentication between the transmitting device and the receiving device, for judging whether the transmitting device and the receiving device are devices that are  
35 allowed to communicate with the transmitting device or not,

on a radio link layer of the radio communications;

5 a first key exchange unit configured to generate a first encryption key and share the first encryption key between the transmitting device and the receiving device when the first authentication between the transmitting device and the receiving device by the first authentication unit is success;

10 a second authentication unit configured to carry out a second authentication between the transmitting device and the receiving device, for protecting copyright of the contents data to be transmitted, through an encrypted radio communication using the first encryption key;

15 a second key exchange unit configured to generate a second encryption key and share the second encryption key between the transmitting device and the receiving device when the second authentication between the transmitting device and the receiving device by the second authentication unit is success; and

20 a communication unit configured to transfer the contents data from the transmitting device to the receiving device through an encrypted communication path which is encrypted by using the second encryption key and provided on the radio link layer.

25 20. A radio communication system, comprising a transmitting device for transmitting copyright protected contents data through radio communications, and a receiving device for receiving the contents data transmitted from the transmitting device, each one of the transmitting device and the receiving device having:

30 a first authentication unit configured to carry out a first authentication between the transmitting device and the receiving device, for judging whether the transmitting device and the receiving device are devices that are allowed to communicate with the transmitting device or not,

on a radio link layer of the radio communications;

5 a first key exchange unit configured to generate a first encryption key and share the first encryption key between the transmitting device and the receiving device when the first authentication between the transmitting device and the receiving device by the first authentication unit is success;

10 a second authentication unit configured to carry out a second authentication between the transmitting device and the receiving device, for protecting copyright pof the contents data to be transmitted, through an encrypted radio communication using the first encryption key;

15 a second key exchange unit configured to generate a second encryption key and share the second encryption key between the transmitting device and the receiving device when the second authentication between the transmitting device and the receiving device by the second authentication unit is success; and

20 a communication unit configured to set up an encrypted communication path which is encrypted by using the second encryption key on the encrypted radio communication which is encrypted by using the first encryption key, and transfer the contents data from the transmitting device to the receiving device through the encrypted communication path.

21. A contents data transfer method in a radio communication system comprising a transmitting device for transmitting copyright protected contents data through  
30 radio communications and a receiving device for receiving the contents data transmitted from the transmitting device, the contents data transfer method comprising:

35 carrying out a first authentication between the transmitting device and the receiving device, for judging whether the transmitting device and the receiving device



are devices that are allowed to communicate with the transmitting device or not, on a radio link layer of the radio communications;

generating a first encryption key and sharing the  
5 first encryption key between the transmitting device and the receiving device when the first authentication between the transmitting device and the receiving device is success;

carrying out a second authentication between the  
10 transmitting device and the receiving device, for protecting copyright of the contents data to be transmitted, through an encrypted radio communication using the first encryption key;

generating a second encryption key and sharing the  
15 second encryption key between the transmitting device and the receiving device when the second authentication between the transmitting device and the receiving device is success; and

transferring the contents data from the transmitting  
20 device to the receiving device through an encrypted communication path which is encrypted by using the second encryption key and provided on the radio link layer.

22. A contents data transfer method in a radio  
25 communication system comprising a transmitting device for transmitting copyright protected contents data through radio communications and a receiving device for receiving the contents data transmitted from the transmitting device, the contents data transfer method comprising:

30 carrying out a first authentication between the transmitting device and the receiving device, for judging whether the transmitting device and the receiving device are devices that are allowed to communicate with the transmitting device or not, on a radio link layer of the  
35 radio communications;

generating a first encryption key and sharing the first encryption key between the transmitting device and the receiving device when the first authentication between the transmitting device and the receiving device is

5 success;

carrying out a second authentication between the transmitting device and the receiving device, for protecting copyright of the contents data to be transmitted, through an encrypted radio communication using the first encryption key;

10

generating a second encryption key and sharing the second encryption key between the transmitting device and the receiving device when the second authentication between the transmitting device and the receiving device is

15 success; and

setting up an encrypted communication path which is encrypted by using the second encryption key on the encrypted radio communication which is encrypted by using the first encryption key, and transferring the contents data from the transmitting device to the receiving device through the encrypted communication path.

20

25

30

35